

Agency Workshop

FedRAMP Compliance and Implementation

March 18, 2013





Welcome

Dave McClure

Associate Administrator

Office of Citizen Services and Innovative Technologies





Session Purpose and Outcomes

- Purpose
 - Detail agency FedRAMP compliance and implementation requirements
- Outcomes
 - Understand FedRAMP its processes, benefits, and key players
 - Ability to explain agency FedRAMP requirements
 - Understand the different FedRAMP assessment paths
 - Clarity on how an agency complies with FedRAMP requirements for existing and planned cloud systems



Agenda

Topic	Speaker	Time
Welcome	Dave McClure	9:00 – 9:10
Cloud and FedRAMP Overview	Katie Lewin	9:10 – 9:20
FedRAMP Responsibilities and Compliance	Maria Roat	9:20 – 9:35
Cloud Inventory	Maria Roat	9:35 – 9:40
Implementation: Planning Phase	Matthew Goodrich	9:40 – 10:10
Questions and Answers		10:10 – 10:30
BREAK		10:30 – 10:40
Implementation: Assessment Phase	Matthew Goodrich	10:40 – 11:10
Implementation: Customer Controls & Authorization	Maria Roat	11:10 – 11:20
Ongoing Assessment & Authorization	Maria Roat	11:20 – 11:30
Wrap-up and Questions and Answers		11:30 – 12:00



Cloud and FedRAMP Overview

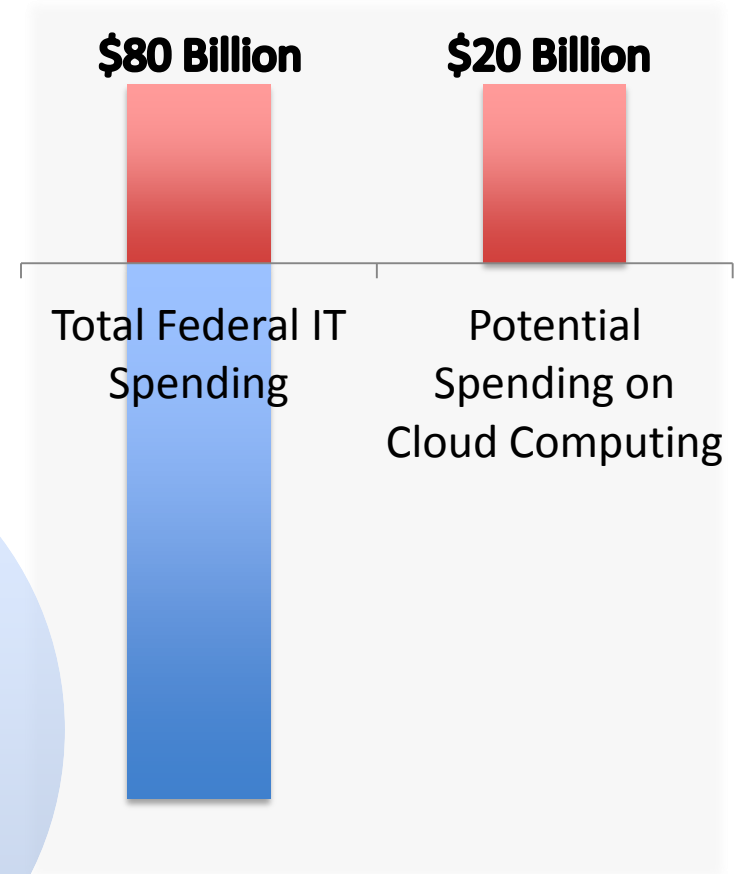
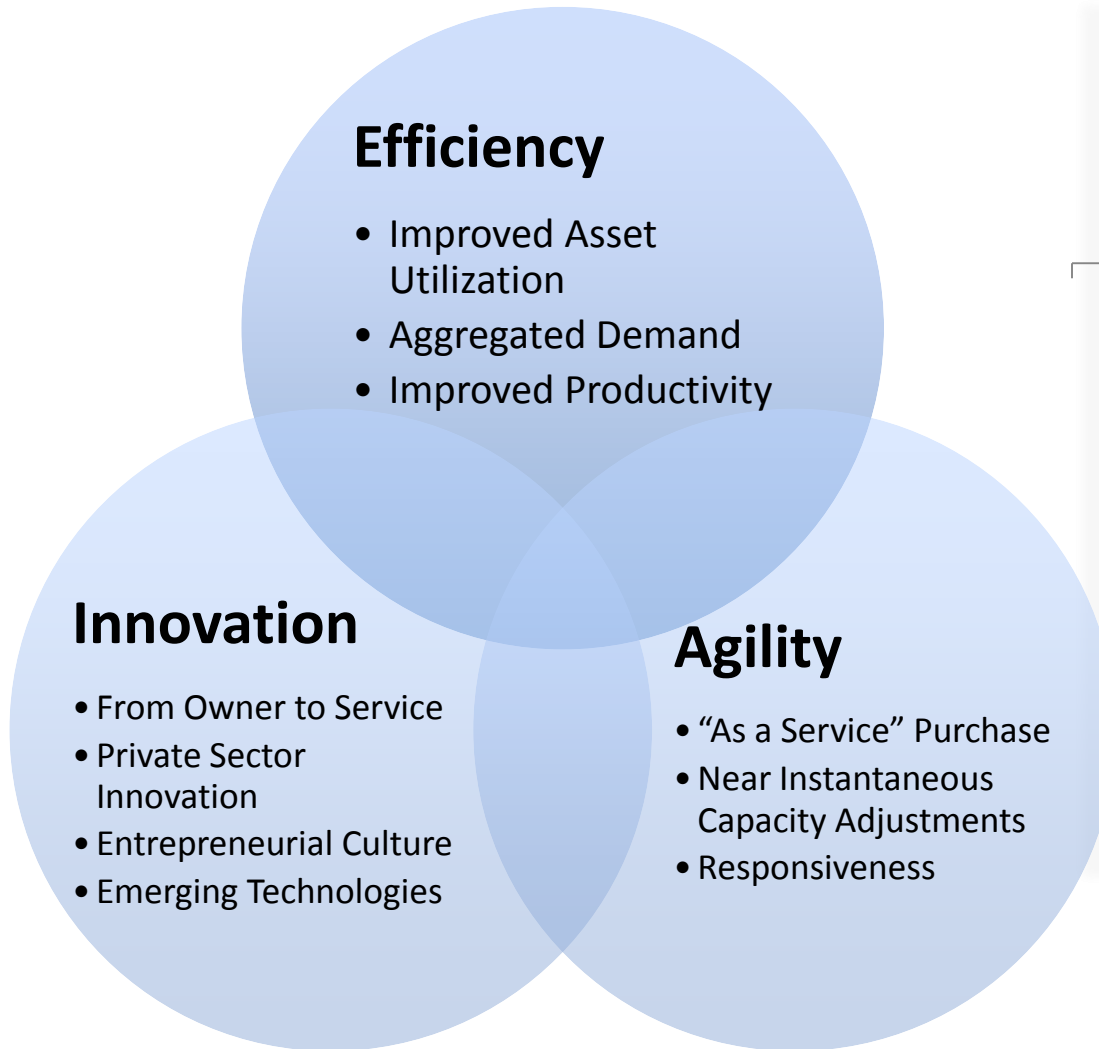
Katie Lewin

Federal Cloud Computing Initiative

Office of Citizen Services and Innovative Technologies



Cloud: A Fundamental Shift in IT





Administration's Drive to the Cloud

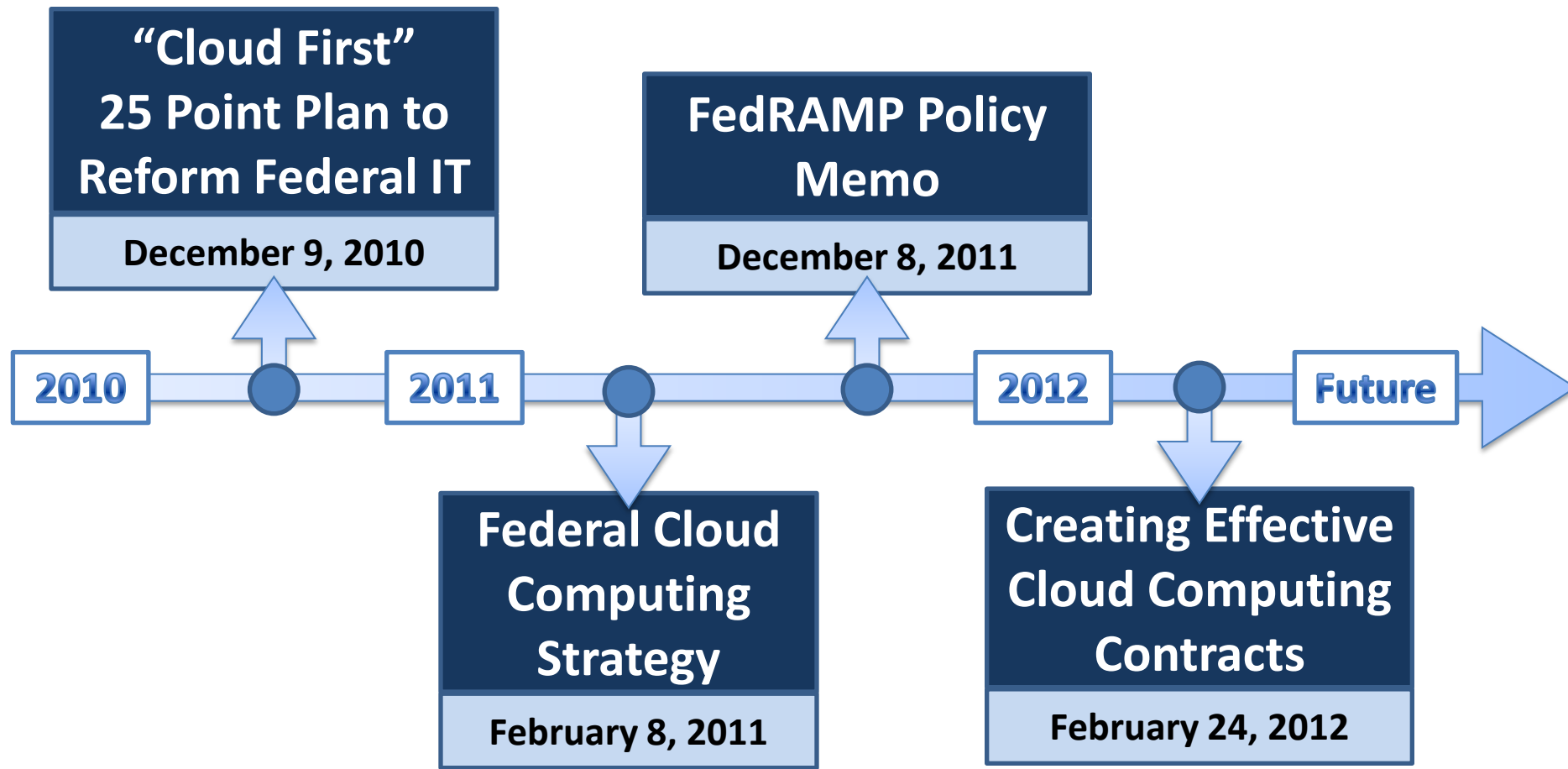
“The Administration’s Federal Cloud Computing Strategy requires agencies to default to cloud-based solutions whenever a secure, reliable and cost-effective cloud option exists – however, the move to the cloud requires a dramatic shift in the way Federal agencies buy IT – from capital expenditures to operating expenditures.

With this shift comes a learning curve as the government analyzes how to best procure this new service-based model. . . .”

***-Steven VanRoekel
U.S. Chief Information Officer, OMB
February 24, 2012***



Federal Timeline for Cloud



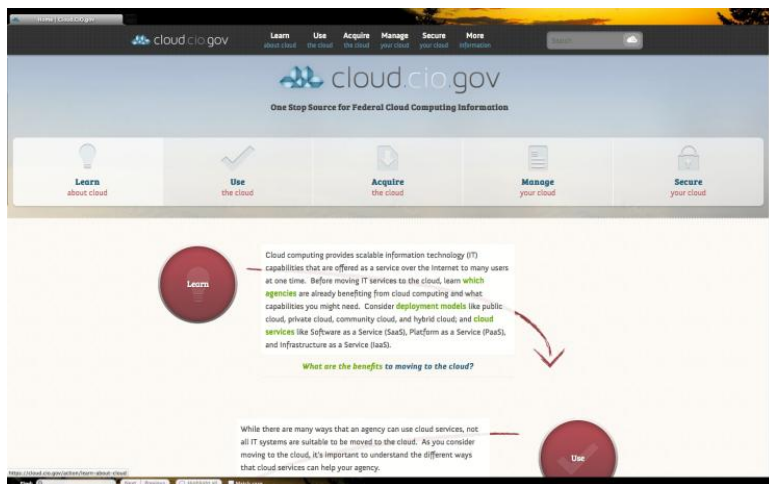


Federal Cloud Computing Program

To foster the adoption of cloud across the Federal government and to address obstacles to cloud adoption



New Information Portal & Collaboration Website



cloud.cio.gov (coming soon)

Blanket Purchase Agreements

- Infrastructure as a Service
- Email as a Service



What is FedRAMP?

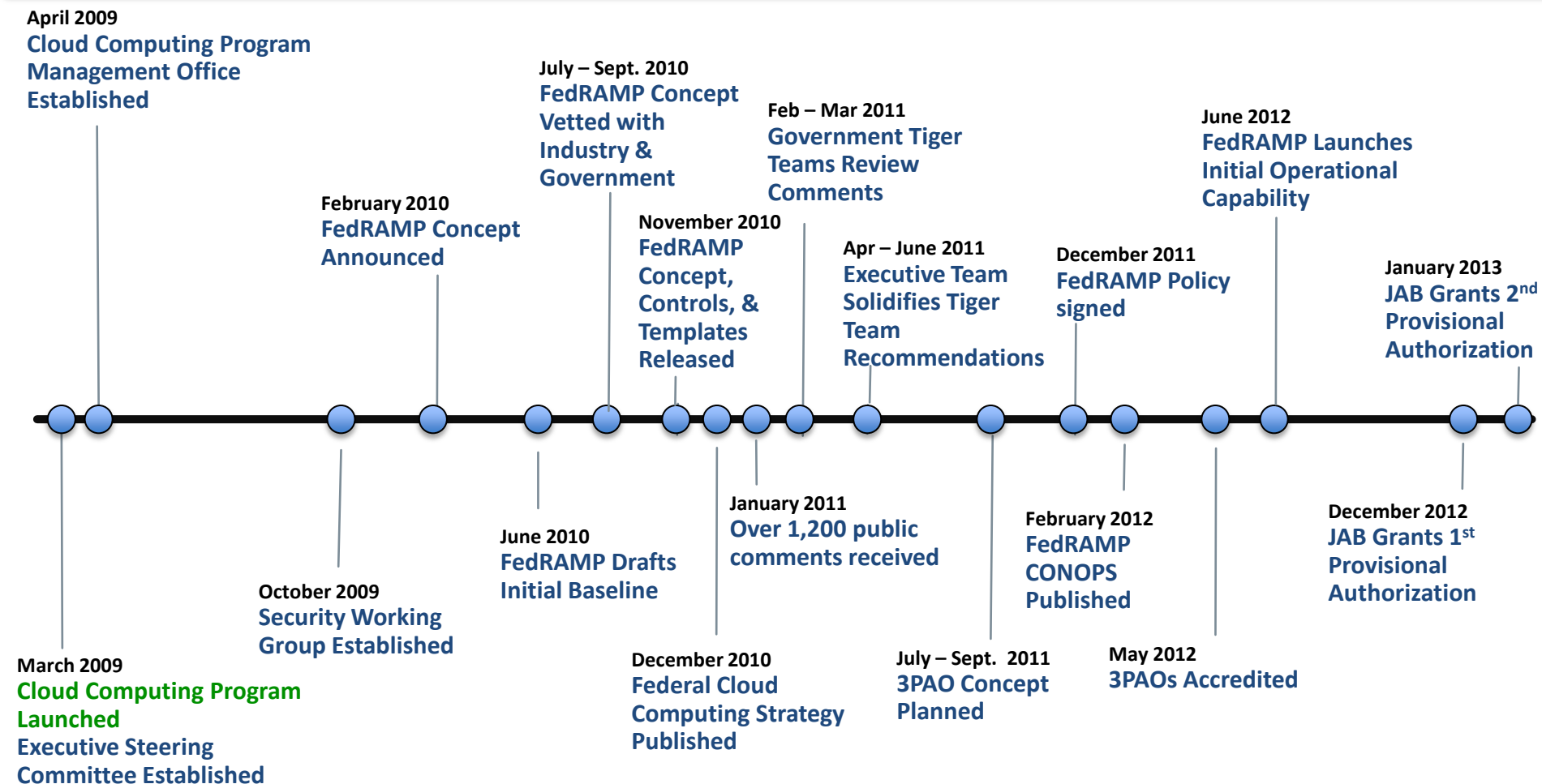
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.





Federal Cloud Computing Initiative and FedRAMP Timeline



Q1 09	Q2 09	Q3 09	Q4 09	Q1 10	Q2 10	Q3 10	Q4 10	Q1 11	Q2 11	Q3 11	Q4 11	Q1 12	Q2 12	Q3 12	Q4 12	Q1 13
-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------



Key Benefits

- Re-use of existing security assessments across agencies
- Savings in cost, time and resources – do once, use many times
- Risk based not compliance based
- Transparency between government and cloud service providers
- Transparency → trust, reliability, consistency, and quality of the Federal security authorization process



FedRAMP Responsibilities & Compliance

Maria Roat
FedRAMP Director
Office of Citizen Services and Innovative Technologies





FedRAMP Policy Memo

December 8, 2011 OMB Policy Memo

- Establishes Federal policy for the protection of Federal information in cloud services
- Describes the key components of FedRAMP and its operational capabilities
- Defines Executive department and agency responsibilities in developing, implementing, operating and maintaining FedRAMP
- Defines the requirements for Executive departments and agencies using FedRAMP in the acquisition of cloud services



FedRAMP Key Players



Federal Agencies

JAB (DOD, DHS, GSA)
PMO- GSA
Technical Advisor – NIST
Continuous Monitoring - DHS

Cloud Service Provider

Provides Cloud IT Services with a provisional authorization granted by FedRAMP JAB



Independent Assessor

Performs initial and periodic assessment of security and privacy controls deployed in Cloud information systems



Responsibilities established by the December 8, 2011 OMB Policy Memo

Responsibilities of Key Parties



Federal Agencies

- Require CSPs to meet FedRAMP requirements via contractual provisions
- Submit security assessment documentation and query FedRAMP repository for existing documentation
- Implement customer responsibility controls
- Establish and implement continuous monitoring plans through incident response and mitigation capabilities



Cloud Service Provider

- Submit application for FedRAMP authorization
- Hire independent third party assessor to perform initial system assessment and on-going monitoring of controls
- Create, submit and maintain authorization packages
- Provide Continuous Monitoring reports and updates to FedRAMP and leveraging agencies

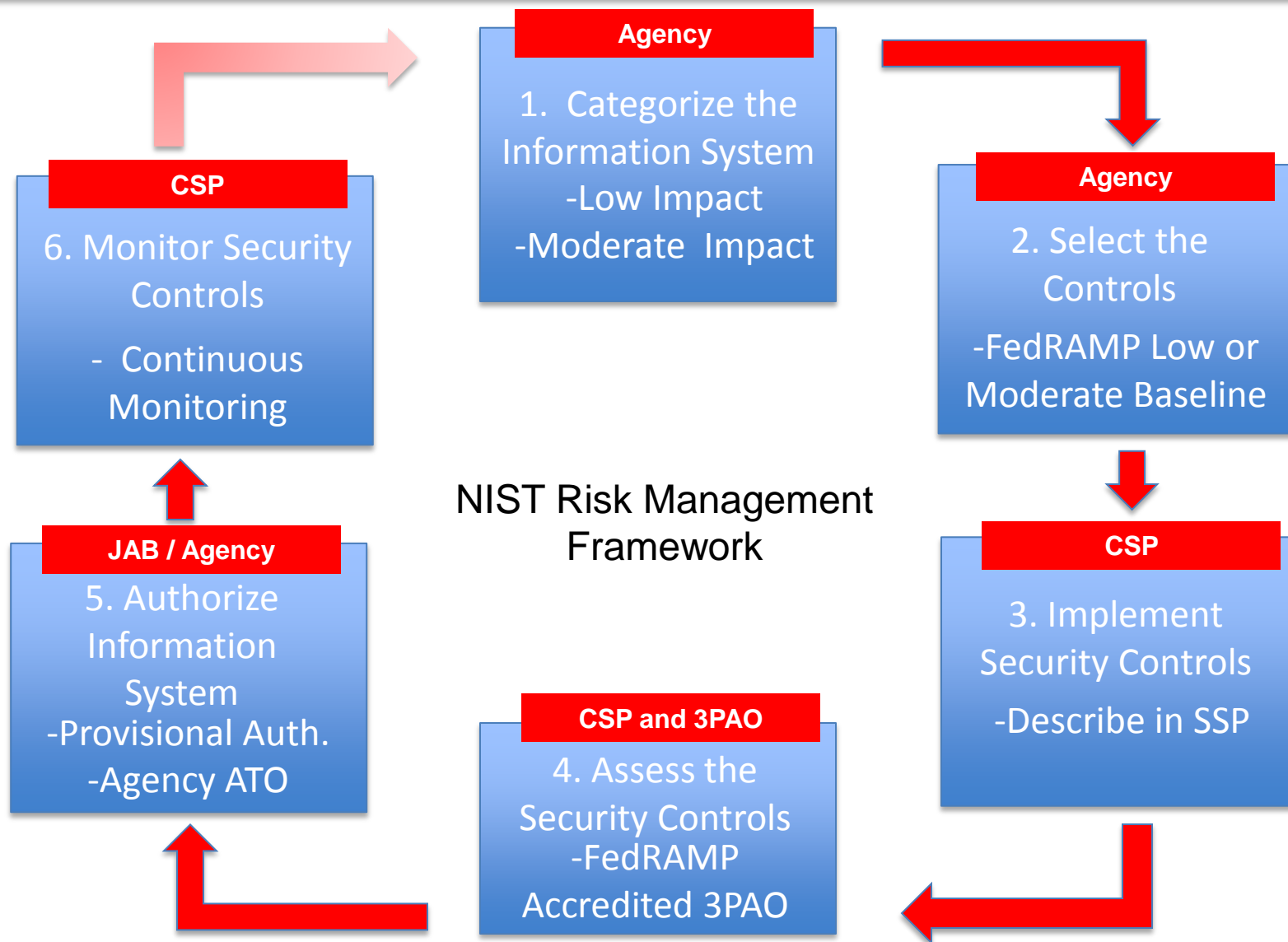


Independent Assessor

- Conduct Assessment of CSP Security Control Implementation
- Generate Security Assessment Reports and associated evidence
- Maintain independence from CSP



FedRAMP Relationship to the NIST Risk Management Framework





Complying with FedRAMP Policy

**All assessments of cloud-based products and services must use the
FedRAMP security requirements:
baseline set of controls and all FedRAMP templates**

- All assessments **do not require** a provisional ATO granted by the JAB
- Agencies can continue to grant their own ATOs without JAB sign-off
- CSPs can submit FedRAMP compliant packages to agencies requesting an ATO
- All assessment documentation must be submitted to FedRAMP PMO for inclusion in the secure repository

**Agencies must leverage existing FedRAMP ATOs
found in the FedRAMP repository**

**June 2014 All Cloud Projects Must Meet
FedRAMP Requirements**



Exception Guidance

- Private cloud deployments
 - Implemented within a Federal facility
 - Operated solely for the use of the Executive Department or Agency
 - Not providing cloud services from the system to any external entities
- Cloud systems at a FIPS 199 Impact Level of High

Bureaus, components or subordinate organizations within an agency are considered external entities

Cloud systems exempt from FedRAMP requirements must continue to comply with FISMA requirements and appropriate NIST security standards and guidelines



Cloud Inventory

Maria Roat
FedRAMP Director
Office of Citizen Services and Innovative Technologies





Conducting the Inventory

- April 2013 Portfolio Stat online data call will gather information on agency cloud deployments
- Agencies will report information on their FIPs 199 low and moderate impact cloud deployments being implemented or planned
 - Agency POC
 - CSP Detail : Name, Service Name, Brief Description, Service Model, Deployment Model, Assessor, FIPS 199 level
 - Implementation detail



FedRAMP Inventory Questions

Fully Implemented

- Do you have an Authority to Operate (ATO) for the system?
- Have you performed a security controls gap analysis against the FedRAMP baseline controls?
- Were FedRAMP requirements met?
- How were FedRAMP requirements met?

FedRAMP Requirements Not Met

- What is the rationale for being unable to meet FedRAMP requirements?
- Have you initiated discussions with the cloud system owner to review missing FedRAMP security controls?
- How do you plan on meeting FedRAMP requirements in the future?
- When will your agency's use of this system be compliant with FedRAMP requirements?



Plans for Cloud Inventory Effort

- Identify synergies between agency cloud portfolios
- Connect organizations using the same cloud service provider (CSP) to provide the same or similar cloud service
- Promote special interest groups of agencies using the same cloud service to establish an organized approach for requesting the CSP implement FedRAMP baseline controls
- Prioritize services to receive a Joint Authorization Board provisional authorization
- Assess FedRAMP applications and documentation received as compared to agency cloud portfolios



FedRAMP Implementation Planning Phase

Matthew Goodrich
FedRAMP Program Manager
Office of Citizen Services and Innovative Technologies





Three Phases of Implementation

Phase	Description
Planning	What path will my agency use to establish or implement a cloud service that is FedRAMP compliant?
Assessment	What is my agency's role in assessing the cloud service?
Customer Controls & Authorization	How does my agency add additional controls and authorize the system?



Planning Phase

Purpose and Key Steps

- Purpose
 - Determine the agency's path for meeting FedRAMP requirements

- Key Steps
 1. Incorporate FedRAMP requirements into contract clauses
 2. Identify if FedRAMP security assessment package available to leverage
 3. Gain access to the FedRAMP secure repository to review security assessment documentation
 4. Determine FedRAMP implementation path
 5. Alert FedRAMP PMO of implementation path



FedRAMP Contract Language

Planning Phase

FedRAMP is the implementation of FISMA and applicable NIST security standards and guidelines, commonly found in existing procurements

FedRAMP contract language available at www.fedramp.gov

Standard Contract Language

- Designed for agencies to leverage for use within cloud procurements
- Templates help agencies address:
 - requirement to be FedRAMP compliant
 - FedRAMP privacy requirements
 - FedRAMP security assessment process requirements
 - authorization of system requirement
 - FedRAMP ongoing assessment and authorization requirement

Control Specific Language

- Agencies should not:
 - govern how the provider's administrative end user accounts are managed or authenticated
 - specify parameters for controls in the FedRAMP baseline, except from the perspective of a consumer's implementation
- Some controls that may need additional clauses

Data Jurisdiction	Audit Retention	Incident Reporting	Personnel Screening
Boundary Protection	Media Transport	Info at Rest	Identification Authentication



FedRAMP Website

Planning Phase



- Website lists CSPs with security assessment documentation available in the FedRAMP secure repository

CSP Name	Service Name	Service Description
ATO Date	Repository Level	3PAO
FIPS 199 Level	Service Model	Deployment Model



Access Secure Repository

Planning Phase

1. Identify package for review based on website listing
2. Complete FedRAMP Package Access Request form
 - Supervisor must signoff on form
 - FedRAMP will provide notification of acceptance or rejection of request
 - Must demonstrate a need to view the package
3. Receive access to OMB MAX folder corresponding to security assessment package for cloud service
 - Access granted on a per person per package basis

FedRAMP Package Access Request Form For Review of FedRAMP Security Package			
INSTRUCTIONS: 1. Please complete this form, then print and sign. 2. Distribute to your Government Supervisor for review and signature. 3. Please email your signed Request Form to info@fedramp.gov .			
User Information			
Date of Request:		Agency or Department:	
First Name:		Bureau:	
Last Name:		Office:	
E-Mail Address:			
Phone:			
Select one:	<input type="checkbox"/> Federal Employee <input type="checkbox"/> Federal Contractor – If yes, what organization?:		
If you are a Federal contractor, please also review Attachment A: Federal Contractor Non Disclosure Agreement for FedRAMP, sign and attach to this request.			
Requested Package			
Name of Package Requested:			
What is the Package ID (located on the CSP listing on FedRAMP.gov)?			
Do you have a current contract with this CSP?			
Contract Number			
Name of CSP Contact:			
Phone:			
Email:			
If you are not a current customer, access is granted for 30 days in order to properly ensure a high level of access control and maintain proper security over the security authorization packages.			
Access Authorization			
All reviewers are required to use multi-factor authentication via PIV (Personal Identity Verification) card to obtain access to the FedRAMP secure repository on the OMB MAX system.			
In order to gain access to the FedRAMP secure repository, the FedRAMP PMO requires approval from an Authorized FedRAMP Approver. This is your agency CISO or someone they have designated. If you are unsure of who your FedRAMP approver is, please email the FedRAMP PMO at Info@FedRAMP.gov .			
Authorized FedRAMP Approver:			
First Name:		Title:	
Last Name:		Agency / Department:	
Phone:		Bureau:	
Email:		Office:	

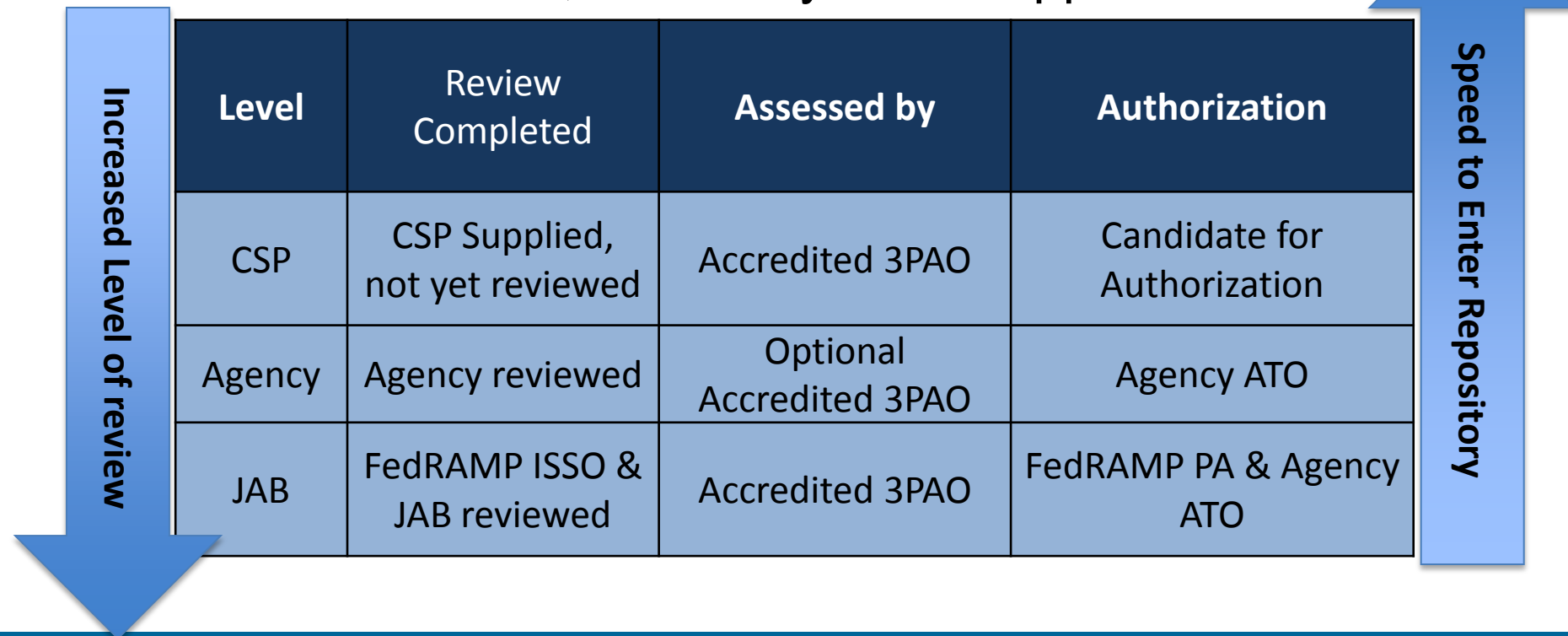


Leverage an Authorization

Planning Phase

FedRAMP maintains a repository of standardized security assessment packages Agencies can leverage to make their own risk-based decisions to grant an ATO for a cloud solution for their Agency.

This repository is key to the
“do once, use many times” approach.





Package Type's Impact on Agency Responsibilities

Planning Phase

Agency Responsibility	Repository level		
	CSP	Agency	JAB
Accept risks and issue authority to operate	√	√	√
Review documentation for both completeness and accuracy	√	√	
Submit annual assessment to the FedRAMP PMO	√	√	
Provide continuous monitoring based on FedRAMP requirements	√	√	Review



Initial Review of Leveraged Documentation

Planning Phase

- **Control Tailoring Workbook (CTW)** and **Control Implementation Summary (CIS)** are good documents to assess the extent to which the cloud solution's security control implementation will meet your agency's needs and ability to leverage corresponding security assessment packages
 - **CTW** – identifies controls that have been adapted by the cloud service provider
 - **CIS** – identifies who is responsible for each security control
- Documents summarize what a customer's responsibility is in securely using a CSPs services as well as what a CSP does to meet FedRAMP security controls



Existing Agency ATO – Migration Path

Planning Phase

- Agency updates existing security assessment to meet FedRAMP requirements

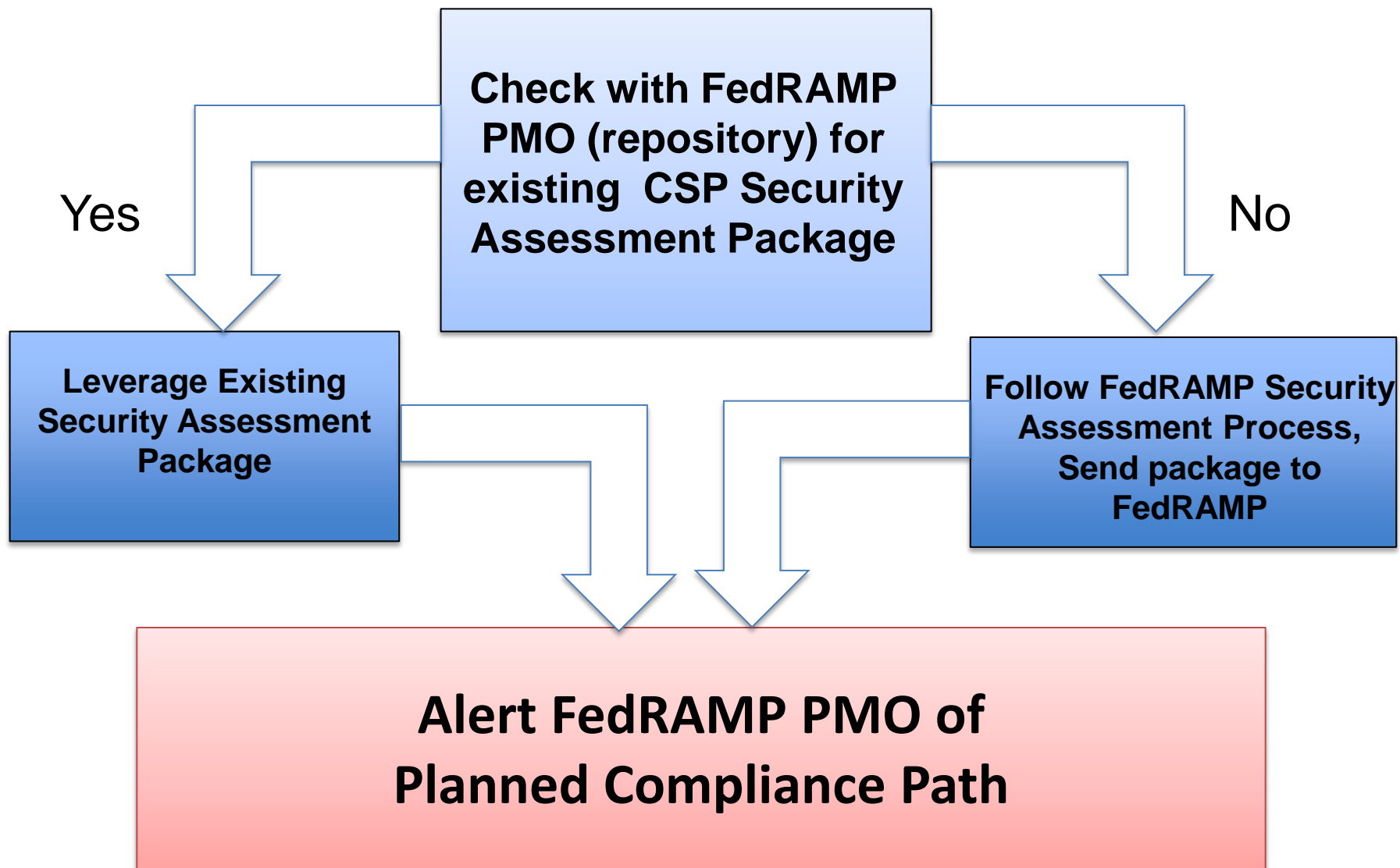
An agency must...

- Provide own resources and bear all costs for the development of the package and ongoing use of the system
- Perform gap analysis of missing controls against the FedRAMP baseline
- Consider modifying existing contract to specifically stipulate FedRAMP Compliance
- Obtain commitment and compliance schedule for CSP to meet FedRAMP control requirements
- Migrate existing security package documents to required FedRAMP templates



Alert FedRAMP PMO

Planning Phase





Questions and Answers





BREAK





FedRAMP Implementation Assessment Phase

Matthew Goodrich
FedRAMP Program Manager
Office of Citizen Services and Innovative Technologies





Assessment Phase

Purpose and Key Steps

- Purpose: Develop or review security assessment documentation required to make a risk-based decision to authorize the cloud service for use at your agency
- Key Steps
 - 1) Document security controls
 - 2) Perform security tests
 - 3) Finalize security assessment package



Document Security Controls

Assessment Phase – Document Controls

1. Understand FedRAMP controls
2. Address and document how the CSP implements each FedRAMP security control
 - Control responsibility
 - What solution is being used for the control
 - How the solution meets the control requirement



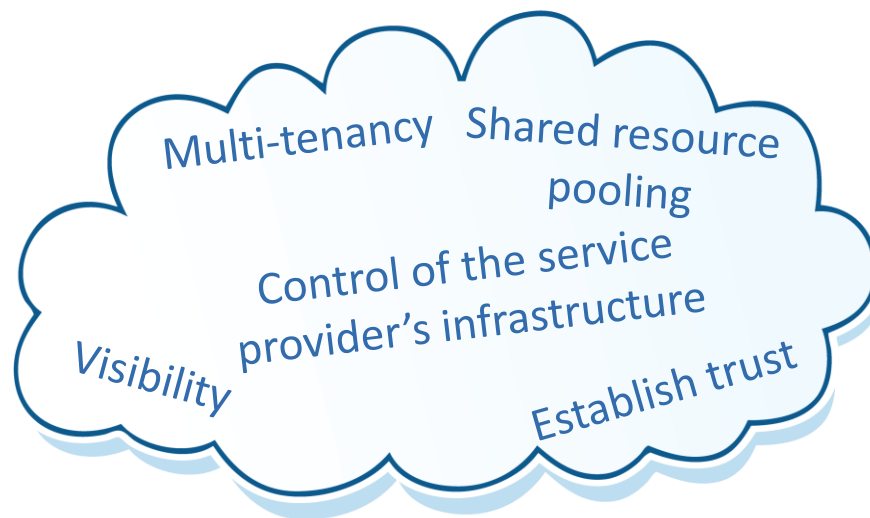
FedRAMP Baseline Security Controls

Assessment Phase – Document Controls

Controls are based upon the NIST SP 800-53 R3 catalog of controls for low and moderate impact systems

Impact level	NIST Baseline Controls	Additional FedRAMP Controls	Total Controls Agreed to by JAB for FedRAMP
Low	115	1	116
Moderate	252	46	298

Additional FedRAMP controls selected to address unique elements of cloud computing



FedRAMP Security Controls Baseline Available on [FedRAMP.gov](https://www.fedramp.gov)




System Security Plan (SSP)

Assessment Phase – Document Controls

- Describes the purpose of the system
- Detailed description of Control Implementation
- Global view of how the system is structured
- Defines roles of the systems users and identifies personnel responsible for system security
- Delineates control responsibility between the customer or vendor
- The SSP is the key document to moving the FedRAMP assessment process forward

System Security Plan
<Information System Name>, <Date>

FedRAMP System Security Plan (Template)







<Vendor Name>

<Information System Name>

<Version 1.0>
October 15, 2012

Company Sensitive and Proprietary
For Authorized Use Only





Reviewing Security Controls in the SSP

Assessment Phase – Document Controls

- Security control section details all the security controls and control enhancements required for FedRAMP
 - Responsible role – maintain and implement the control
 - Parameter of control – frequency
 - Implementation Status
 - Control origination – organization responsible for implementing and managing the control (vendor, customer, shared)
 - Solution and how implemented

13.7.2 User Identification and Authentication (IA-2)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IA-2	Control Summary Information
Responsible Role:	
Parameter:	
Implementation Status (check all that apply): <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	
Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing Provisional Authorization (PA) for <Information System Name>, <Date of PA>	
IA-2 What is the solution and how is it implemented?	



SSP Supporting Documentation (1/2)

Assessment Phase – Document Controls

- **Information Security Policies** –CSP's Information Security Policy that governs the system described in the SSP
- **User Guide** - describes how leveraging agencies use the system
- **Rules of Behavior** - defines the rules that describe the system user's responsibilities and expected behavior with regard to information and information system usage and access
- **Configuration Management Plan** - describes how changes to the system are managed and tracked (consistent with NIST SP 800-128)



SSP Supporting Documentation (2/2)

Assessment Phase – Document Controls

- **IT Contingency Plan** - details how the recovery of the system occurs in the case of a disruption of service
- **Incident Response Plan** – explains provider actions in response to a security incident
- **Privacy Threshold Analysis** - questionnaire used to help determine if a Privacy Impact Assessment is required
- **Privacy Impact Assessment** - assesses what Personally Identifiable Information (PII) is captured and if it is being properly safeguarded



Perform Security Tests

Assessment Phase – Perform Security Tests

1. Assess against the SSP with NIST SP 800-53a test cases
2. Independent Assessor audits assessment and results
3. Independent Assessor generates security assessment report



Role of the Independent Assessor

Assessment Phase – Perform Security Tests

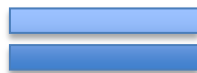
- Develops Security Assessment Plan (SAP)
- Performs Initial and Periodic Assessments of CSP Security Controls
- Conducts Security Testing
 - Use Test Case Workbooks
 - Manual Tests
 - Automated Tests
- Develops Security Assessment Report (SAR)
- Assessor must be independent
 - Cannot test and help CSP prepare documents
 - Cannot test and assist CSP in implementing controls



Independent Assessor Conformity

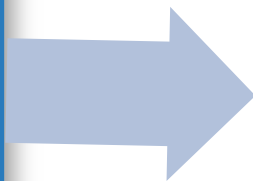
Assessment Phase – Perform Security Tests

**Third Party Assessment
Organization (3PAO)**



**Accredited Independent
Assessor**

**Benefits of leveraging
an accredited
independent assessor
(Third Party
Assessment
Organization – 3PAO)**



**Creates consistency in security
assessments in accordance
with FISMA and NIST standards**

- Ensures assessor independence from CSP in accordance with international standards
- Establishes an approved list of assessors - 3PAOs for CSPs and agencies to choose from to satisfy FedRAMP requirements.



Third Party Assessment Organizations

Assessment Phase – Perform Security Tests



The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Are you a...?

Federal Agency



What can FedRAMP do for your agency?

CSP Cloud Service Provider



Get a FedRAMP security authorization.

3PAO Third Party Assessors



Become a FedRAMP accredited assessor.

FEDRAMP HAS NOW LAUNCHED

To apply or sponsor a system for authorization, please fill out the FedRAMP application [here](#).

CONTACTS

General Inquiries
info@fedramp.gov

Press Inquiries
202-501-9113

KEY LINKS

[FedRAMP Initiation Request](#)

[Accredited 3PAOs](#)

[Authorized CSPs](#)

KEY DOCUMENTS

[FedRAMP Concept of Operations \(CONOPS\)](#)

[FedRAMP Security Controls](#)

[FedRAMP Templates](#)

[FedRAMP Continuous Monitoring Strategy Guide](#)

[FedRAMP Standard Contract Clauses](#)

[FedRAMP Control-Specific Contract Clauses](#)

[Guide to Understanding FedRAMP](#)

[FedRAMP Policy Memo \(OMB\)](#)

[3PAO Program Description](#)

[FedRAMP JAB Charter](#)

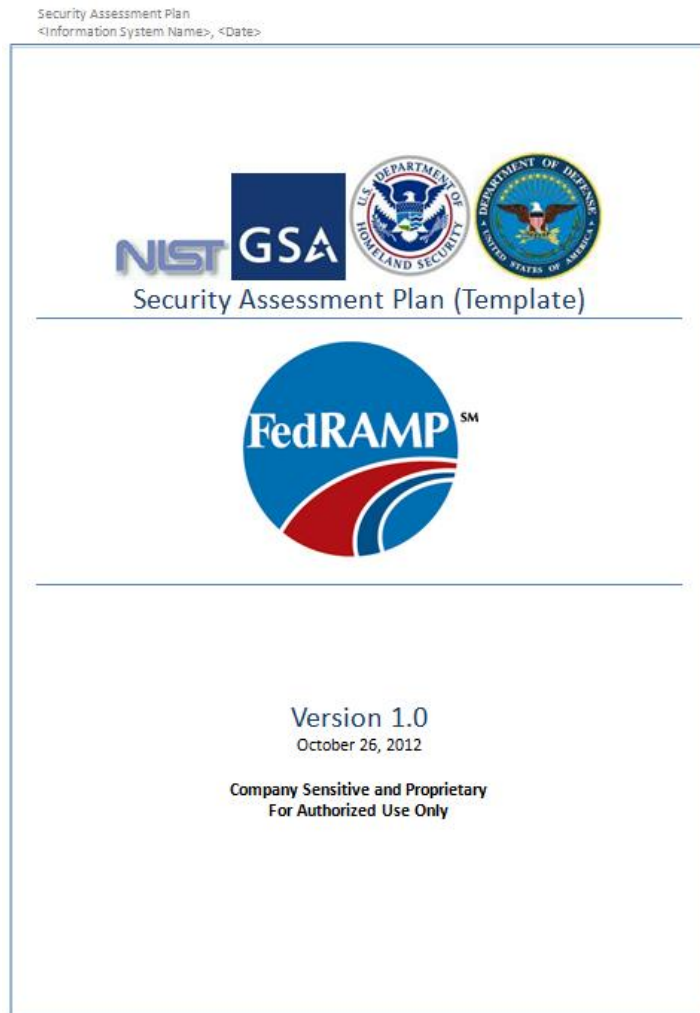
Accredited 3PAOs

BrightLine	Homeland Security Consultants
COACT, Inc.	J.D. Biggs and Associates, Inc.
Coalfire Systems	Knowledge Consulting Group, Inc.
Department of Transportation (DOT) Enterprise Service Center (ESC)	Logyx LLC
Dynamics Research Corporation (DRC)	Lunarline, Inc.
Earthling Security, Inc.	Secure Info
Electrosoft Services, Inc.	SRA International, Inc.
	Veris Group, LLC



Security Assessment Plan (SAP)

Assessment Phase – Perform Security Tests



- Independent Assessor develops the SAP
- Defines scope of assessment
 - Hardware
 - Software
 - Databases
 - Applications
 - Facilities
- Testing Schedule
- Rules of Engagement (ROE)
 - Components included and excluded in assessment
 - Rules for transmission of results
 - ROE signed by CSP and Independent Assessor



Security Assessment Report (SAR)

Assessment Phase – Perform Security Tests

Security Assessment Report
<Information System Name>, <Date>



<Vendor Name>

<Information System Name>

<Sensitivity Level>

December 3, 2012

Company Sensitive and Proprietary
For Authorized Use Only

- Independent Assessor develops the SAR
- Documents findings
- Analysis of test results
- Highlights ways for CSPs to mitigate security weaknesses
- Primary document for making risk-based decisions



Finalize Security Assessment

Assessment Phase – Finalize Assessment

1. CSP develops plan of actions and milestones (POA&M)
2. CSP declares conformity with FedRAMP requirements and submits security assessment package



Plan of Action and Milestones

Assessment Phase – Finalize Assessment

- Detailed plan with a schedule of how the CSP plans to address and fix and vulnerabilities found during testing
- All SAR findings must map to a POA&M item
- False positives marked in the SAR but not identified in the POA&M – as there is no remediation needed to correct false positives.
- CSPs applying for Provisional ATO:
 - Remediate high severity findings before Provisional ATO is granted
 - Remediate moderate findings within 90 days



Declaration of Conformity

Assessment Phase – Finalize Assessment

FedRAMP Self-Attestation

Self-Attestation Letter & Template



Version 1.0

July 27, 2012

Company Sensitive and Proprietary

Page 1

- CSP attests and verifies that the system conforms to FedRAMP requirements.
- Certifies that all controls are working properly
- Both JAB and leveraging agencies use the Self-Attestation Declaration of Conformity when considering issuing an ATO



Complete Assessment Package

Assessment Phase – Finalize Assessment

- A complete security authorization package includes deliverables in section 10 of the FedRAMP CONOPS

- Mandatory Templates:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report

- Other Templates located on fedramp.gov:

- Control Tailoring Workbook
- Control Implementation Summary
- IT Contingency Plan
- Plan Of Action & Milestones
- Supplier's Declaration of Conformity



FedRAMP CONOPS

10. Deliverables

Deliverables noted in Table 10-1 must be created using the FedRAMP templates. All deliverable templates are available on www.FedRAMP.gov.

Table 10-1. FedRAMP Deliverables by Process Area

Process Area	Deliverable	Description
Security Assessment Process Area, Initiate Request Process	FedRAMP Request Form	The FedRAMP request form is used by Federal agencies and CSPs to request initiation of the FedRAMP security assessment process.
	FIPS 199 Categorization	The FIPS 199 Security categorization is used to determine the impact level to be supported by the cloud information system/service. The provider should categorize based on the system data currently stored and not leveraging agency data to be hosted on their system.
	Control Tailoring Workbook	This document is used by CSP to document their control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls.
	Control Implementation Summary	This document summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency.
Security Assessment Process Area, Documenting Security Controls	System Security Plan (SSP)	The SSP describes how the controls are implemented within the cloud information system and its environment of operation. The SSP is also used to describe the system boundaries.
	Information Security Policies	The CSP's Information Security Policy that governs the system described in the SSP.
	User Guide	The User Guide describes how leveraging agencies use the system.
	Rules of Behavior	This document is used to define the rules that describe the system user's responsibilities and expected behavior with regards to information and information system usage and access.
	IT Contingency Plan	These documents define and test interim measures to recover information system services after a disruption. The ability to prove that system data can be routinely backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts.
	Configuration Management Plan	This plan describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128.



FedRAMP Implementation

Customer Controls and Authorization Phase

Maria Roat
FedRAMP Director
Office of Citizen Services and Innovative Technologies





Customer Controls & Authorization Phase

Purpose and Key Steps

- Purpose: Review security assessment documentation and grant authority to operate
- Key Steps
 1. Review FedRAMP security authorization package
 2. Implement customer controls
 3. Grant authorization
 4. Alert FedRAMP PMO of authorization granted and provide feedback regarding additional controls used



Customer Review of Authorization Package

Customer Controls & Authorization Phase

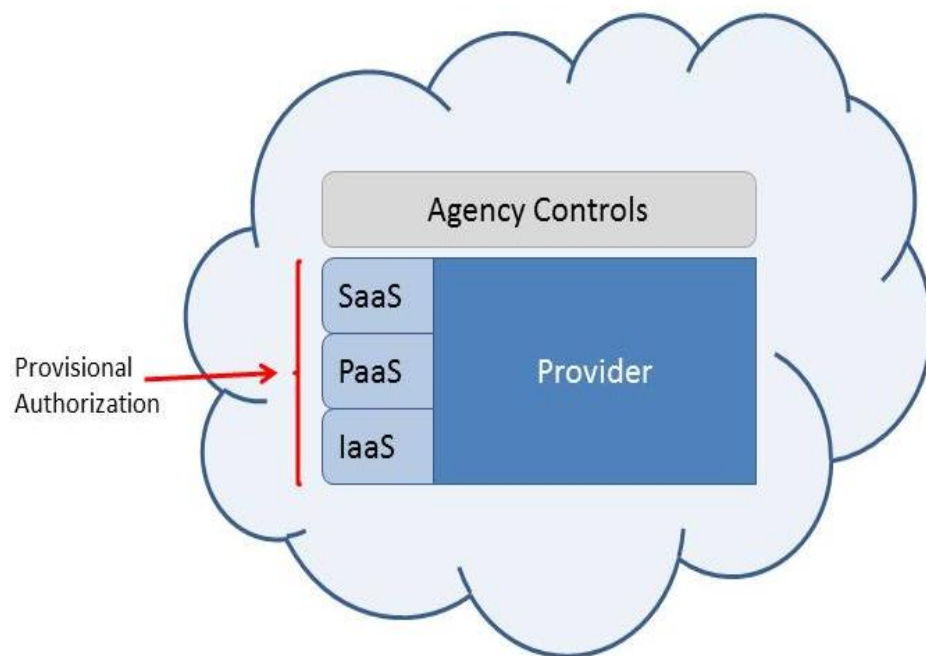
- Security Authorization Package
 - Complete, consistent, and compliant with FedRAMP policy
 - Hardware or software inventory included
 - Content addresses the who, what, when, and how
 - Delivery of supporting documentation and information adequately referenced
 - Non-applicable controls not presented as implemented
- Risk review of Security Assessment Report and current Plan of Actions and Milestones

- Include controls added on to FedRAMP baseline
- Include controls for applications & middleware
- Include controls with agency shared responsibility

Shared Responsibility

Both the CSP and the agency use two-factor authentication for authenticating to privileged and non-privileged accounts.

Both CSP and agency must ensure users take security awareness training.





Authorize System

Customer Controls & Authorization Phase

- Agencies make own risk-based determination for granting Authority to Operate



- Submit final security assessment package to FedRAMP PMO if not already in the secure repository
- Notify FedRAMP PMO if Agency ATO withdrawn



FedRAMP Ongoing Assessment & Authorization

Maria Roat
FedRAMP Director
Office of Citizen Services and Innovative Technologies





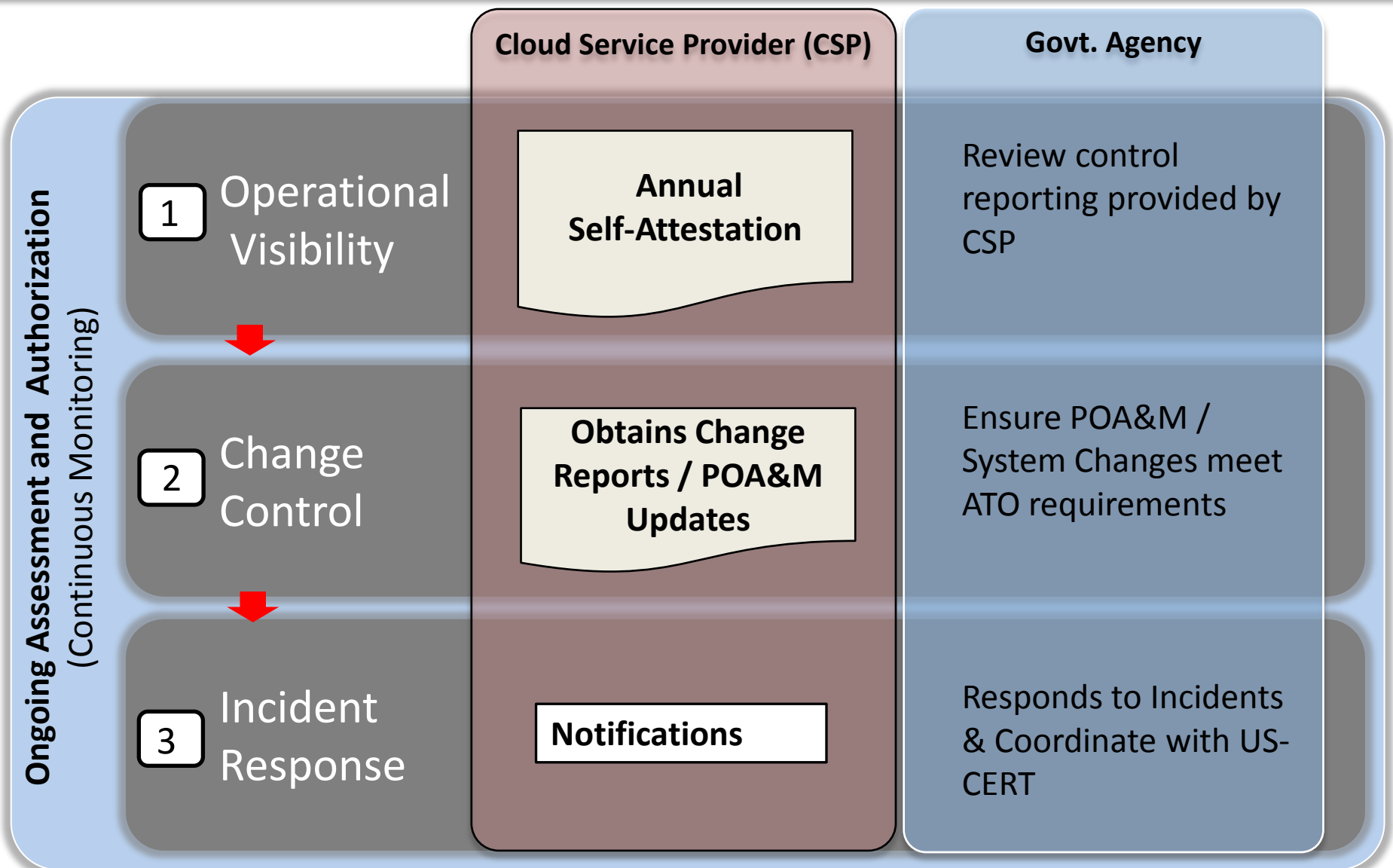
Ongoing Assessment and Authorization

- Purpose: Determine whether deployed security controls remain effective in light of planned and unplanned changes that occur in the system and its environment over time.
- Key Steps
 1. Review of control implementation
 2. Review changes to the system
 3. Monitor incidents and new vulnerabilities



Overview

Ongoing Assessment & Authorization





Operational Visibility

Ongoing Assessment & Authorization

CSPs

- CSP submits artifacts to the FedRAMP ISSO as defined by the FedRAMP Continuous Monitoring Strategy and Guide
- Artifacts include POA&Ms, Scans, and the Annual Self Attestation

FedRAMP

- The ISSOs monitor POA&Ms and reporting artifacts (vulnerability scan reports)
- Artifacts are stored in the Secure Repository
- ISSOs provide the JAB and leveraging agencies with updated information on the system so that risk-based decisions can be made about ongoing authorization

Agency

- Review artifacts in the Secure Repository to ensure that the risk posture of the CSP falls within agency tolerance
- Monitor security controls that are agency responsibilities

CSP Submission Schedule	Number of Deliverables
Monthly	1
Quarterly	2
Semi-Annually	1
Annually	10
Every 3 Years	1



Change Control

Ongoing Assessment & Authorization

CSPs

- CSPs must notify FedRAMP of any planned significant changes to the system before implementing the change
- CSPs must submit an updated SAR 30-days after implementation

FedRAMP

- Changes are reviewed by FedRAMP ISSOs and approved by the JAB
- FedRAMP will notify leveraging agencies:
 - If a significant change is planned and when it occurs
 - If it affects security posture or adds unacceptable levels of risk

Agency

- Upon notification of a significant change agencies should inform FedRAMP if they believe the planned changes will adversely affect the security of their information
- Agencies should review the change following the implementation of an approved change

The image shows a screenshot of the 'FedRAMP Significant Change Security Impact Assessment Form'. The form is titled 'FedRAMP Significant Change Security Impact Assessment Form' and includes the FedRAMP logo. It contains several sections: 'INSTRUCTIONS' (1. Please complete this form, then print and sign. 2. Email a scanned copy of the form to your assigned FedRAMP ISSO), 'CSP Contact Information' (Company Name, First Name, E-Mail Address, FedRAMP Assessment Package Number, Last Name, Phone), 'Provide the following for the FedRAMP accredited SPAO that performed testing as part of the impact assessment.' (SPAO Company Name, First Name, E-Mail Address, Last Name, Phone), 'Type of Change' (a grid of checkboxes for various change types), 'Change Details (please attach additional pages if necessary):', 'Signature:', and 'For FedRAMP PMO Use Only' (Approved: Yes / No, Date).



Incident Response

Ongoing Assessment & Authorization

- **Multiple incident response notification scenarios based on first responder to incident (Refer to the FedRAMP Incident Communication Plan)**

Agency Responsibilities for Incident Response:

- Provide a primary and secondary POC to CSPs and US-CERT
- Notify US-CERT when a CSP reports an incident
- Work with CSPs to resolve incidents by providing coordination with US-CERT
- Notify CSPs, if the agency becomes aware of an incident that a CSP has not yet reported
- Notify FedRAMP ISSO of CSP incident activity
- Monitor security controls that are agency responsibilities.





Agency Responsibilities – JAB vs. Other Paths

Ongoing Assessment & Authorization

Review Level	Description	Authorization	Responsibility for Continuous Monitoring
CSP	CSP Supplied, not yet reviewed	Candidate for Authorization	None
Agency	Reviewed by agency (*Accredited 3PAO Optional)	Agency ATO	Agency
JAB	Reviewed by FedRAMP ISSO & JAB	FedRAMP PA & Agency ATO	FedRAMP



Wrap-Up





Cloud System Compliant with FedRAMP

- The system security package has been created using the required FedRAMP templates
- The systems meets the FedRAMP security control requirements
- The system has been assessed by an independent assessor
- A Provisional Authorization, and/or an Agency ATO, has been granted for the system
- An authorization letter for the system is on file with the FedRAMP PMO



Common Agency Questions

- Do I need to have the JAB grant a Provisional Authorization to be FedRAMP Compliant?
 - No, an agency can grant an ATO using the FedRAMP Controls and templates.
- If an agency wishes to grant their own ATO using the FedRAMP process, must the CSP use an accredited 3PAO?
 - No, but the JAB will only grant Provisional Authorizations if an accredited 3PAO performs the assessment.
- If an agency is starting an acquisition, what must be included in the solicitation?
 - Sample contract clauses are located on [FedRAMP.gov](https://www.fedramp.gov).
- If an agency leverages a FedRAMP authorization, must the agency still grant an ATO?
 - Yes, the agency must implement the consumer controls and grant an ATO for the entire information system.
- Does an agency need to report the FedRAMP system in their FISMA reporting?
 - The agency needs to include its Information System in the FISMA inventory.



Questions and Answers





For more information, please contact us or visit us the following website:

www.FedRAMP.gov

Email: info@fedramp.gov

Follow us on [twitter](#) @ FederalCloud